James E. Cecchi
CARELLA BYRNE CECCHI
BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
Tel: (973) 994-1700
jcecchi@carellabyrne.com

Counsel for Plaintiff and the Proposed Class
[*Additional Counsel Listed On Signature Page*]

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

ALEC WRAY, Individually And On Behalf Of All Others Similarly Situated, Plaintiff, v. AMERICAN NEIGHBORHOOD MORTGAGE ACCEPTANCE COMPANY, LLC D/B/A ANNIEMAC HOME MORTGAGE, Defendant.	Civil Action No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR A JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff, Alec Wray, individually (hereinafter, "Plaintiff"), and on behalf of all others similarly situated ("the proposed Class Members"), and brings this Class Action Complaint against Defendant, American Neighborhood Mortgage Acceptance Company, LLC d/b/a AnnieMac Home Mortgage ("Defendant" or

"AnnieMac"), and alleges, upon personal knowledge as to his own actions and his counsel's investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This putative class action arises out of the failures of Defendant to properly secure and safeguard the Personally Identifying Information[1] ("PII") of at least 171,074 its customers, including Plaintiff and the proposed Class Members, resulting in the unauthorized disclosure of that PII to cybercriminals in a data breach from August 21, 2024, to August 23, 2024 (the "Data Breach").[2]

2. On information and belief, the PII unauthorizedly disclosed in the Data Breach includes at a minimum Plaintiff's and the proposed Class Members' names and Social Security numbers.[3]

3. This Data Breach differs from many in that a portion of the individuals whose PII was compromised in the cyberattack were not customers of Defendant, but whose PII was collected by AnnieMac nevertheless.

4. Headquartered in Mount Laurel, New Jersey, AnnieMac "is a

[1] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).
[2] *See Notice of Security Incident*, (November 14, 2024), attached as **Exhibit A.**
[3] *See Id.*

nationwide mortgage loan provider dedicated to the principle of service — to [its] clients, [its] employees, and [its] business partners."[4]

5. Defendant failed to undertake adequate measures to safeguard the PII of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

6. Further although Defendant states that it discovered the Data Breach on August 23, 2024, AnnieMac waited until November 2024 to notify Plaintiff and the Class, preventing them from taking appropriate measures to mitigate the effects of the Data Breach and the compromise of their PII therein and the resulting harms.

7. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive PII and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class have suffered widespread injury and damages necessitating Plaintiff to seek relief on a class wide basis.

PARTIES

8. Plaintiff is a natural person and citizen of the State of Idaho, who resides in Boise, Idaho in Ada County, where he intends to remain.

9. Defendant is a limited liability company organized and existing under the laws of the State of Delaware, with a principal place of business at 700 East Gate

[4] https://www.linkedin.com/company/anniemac-home-mortgage.

Drive, Mount Laurel, New Jersey 08054 in Burlington County.

JURISDICTION AND VENUE

10. The Court has general subject matter jurisdiction over this civil action under the Class Action Fairness Act, 28 U.S.C. § 1332(d) because the amount in controversy is more than $5,000,000 and minimal diversity exists. Specifically, on information and belief, the Data Breach affected at least 171,074 persons. Moreover, minimal diversity exists because Plaintiff is a citizen of Idaho and Defendant, on information and belief, is a citizen of New Jersey.

11. This Court has personal jurisdiction over Defendant because AnnieMac's headquarters is in this State.

12. Venue is proper in this Court because a substantial portion of the events giving rise to this Action occurred in this District.

FACTUAL BACKGROUND

A. Defendant, AnnieMac

13. Defendant is a private mortgage loan company, based in New Jersey, which operates branches in Boise, Idaho; Anchorage, Alaska; Casa Grande, Arizona; Chula Vista, California; in Danielson, Unionville, and Vernon, Connecticut; in Newark and Rehoboth Beach, Delaware; Atlanta Georgia; Oak Brook, Illinois; in Warsaw and Indianapolis, Indiana; at Delray Beach, Orlando, Palm Coast, and Ponte Vedra, Florida; in Portland, Maine; at Annapolis, North Bethesda, and Waldorf,

Maryland; at Middleboro and Waltham, Massachusetts; in Eden Prairie, Minnesota; in Kansas City, Missouri; in Reno, Nevada; at Bedford and Nashua, New Hampshire; at numerous locations in New Jersey, including in Mount Laurel, East Brunswick, Fairfield, Forked River, Keyport, Lyndhurst, Netcong, Sewell, Sparta, Toms River, and Wall, New Jersey; in Albany, Melville, and in Rochester, New York; in Cincinnati, Columbus, and Montgomery, Ohio; in Blue Bell and York, Pennsylvania; in Providence and Warwick, Rhode Island; in Greenville, South Carolina; in Plano, San Antonio, and Spring, Texas; and at Virginia Beach, Virginia.[5]

14. At its many locations, Defendant provides myriad financial home mortgage services, including: conventional loans; U.S. Veterans Administration (VA) loans; U.S. Department of Agriculture (USDA) loans; Federal Housing Administration (FHA) loans; as well as "Jumbo Loans" ("…a type of mortgage that is used to finance homes that are too expensive for a traditional conventional loan," usually in excess of "the local conforming limit, which in most cases is $647,200[,]") and Renovation Loans.[6]

15. In addition, AnnieMac provides other specialized mortgage products and programs:

- AnnieMac Cash2Keys ("With our Cash Offer program, even the

[5] https://www.annie-mac.com/branch.
[6] https://www.annie-mac.com/page/more-options.

odds and get your offers accepted, all with the power of cash. With Buy Now, Sell Later, current homeowners can comfortably sell their old home all while securing a new one.");

- Access Your Home's Equity ("As you start to make payments on your mortgage, you gain equity in your home. Take advantage of the equity you have built up over time and receive cash from equity built.");
- OneUp ("AnnieMac Home Mortgage's OneUP program provides homebuyers the option to make a minimal 1% down payment to secure a home, while we provide an additional 2% or $2000 lender grant towards their down payment.");
- Rate Relief ("In a market where timing is everything, a rate buydown can significantly lower the monthly mortgage payments for a future homeowner. By reducing the mortgage rate with Rate Relief, you're effectively lowering the cost of owning your home.");
- Temporary Buydown ("A temporary mortgage interest rate buydown is a home financing strategy that home buyers can use to temporarily lower their interest rate to make their monthly mortgage payments more affordable."); and,

- Purchase Protection Program ("Choose the right time to refinance to a potentially lower interest rate. The Purchase Protection Program is valid on first lien, purchased before 12/31/2024 or refinance with us before 12/31/2025.").[7]

16. On information and belief, AnnieMac generates annual revenue of $241.7 million per year.[8]

17. As a condition of providing financial and mortgage loan services, Defendant required that its customers, including Plaintiff and the Class Members, provide AnnieMac with their PII, including their names and Social Security Numbers.

18. Defendant stored these customers' PII in its information technology computer systems and servers, on information and belief located at its headquarters in Mount Laurel, New Jersey.

19. On information and belief, the information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

20. In collecting and maintaining PII, Defendant agreed it would safeguard that customer data in accordance with its internal policies and industry standards.

[7] *Id.*
[8] https://growjo.com/company/AnnieMac_Home_Mortgage#google_vignette (last visited Dec. 12, 2024).

After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

21. Defendant made promises and representations to Plaintiff and Class Members that their PII would be kept safe and confidential, and that the privacy of that information would be maintained, including in its privacy policies.

22. Annie Mac has stated that "…the confidentiality, privacy, and security of personal information with [its] care are among AnnieMac's highest priorities."[9]

23. AnnieMac maintains a Privacy Policy, posted on its website, in which it states, "During the course of processing your application, we accumulate non-public personal financial information from you and from other sources about your income, your assets, and your credit history in order to allow a lender to make an informed decision about granting you credit."[10]

24. Defendant goes on to describe the information, including PII, it collects, *to wit*:

We collect non-public information about you from the following sources:

- Information we receive from you on applications or other forms
- Information about your transactions with us, our affiliates, or others
- Information we receive from a consumer reporting agency
- Non-personally identifiable information about you in a number of ways, including tracking your activities through your IP

[9] Notice of Data Security Incident, Exhibit A.
[10] Privacy Policy, https://www.annie-mac.com/page/privacy (last visited Dec. 12, 2024), attached as **Exhibit B.**

address or most-recently-visited URL

- Personally identifiable information when you voluntarily submit contact information to us, such as name, phone, email address, and mailing address by filling out a form or survey, registering your email address with us or emailing us
- We may also collect personal information from you at other points on our site that state that personal information is being collected.[11]

25. In its Privacy Policy, Defendant specifically represents and promises to its customers, including Plaintiff and the Class Members, that, "**[w]e restrict access to nonpublic personal information about you to those employees who need to know that information to provide products or services to you. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information**."[12]

26. Indeed, Defendant states in its Privacy Policy that, "We use industry-standard methods to protect your personally identifiable information from unauthorized access. Among other techniques, we usually store such information on a computer behind our 'firewall' in a secure location, and we often restrict the number of employees internally who can access such data…"[13]

27. Moreover, therein, Defendant enumerates the purposes for which it may user customers' PII, including to perform services, "…as required by law and when

[11] *Id*.
[12] *Id*. (bold emphasis added).
[13] *Id*.

we believe that disclosure is necessary to protect our rights and/or comply with a judicial proceeding, court order, or legal process served on our Web site."[14]

28. The Data Breach that came to pass due to Defendant's failures to protect Plaintiff's and the Class Members' PII is not included in the purposes for which AnnieMac may disclose its customers PII, as stated in the Privacy Policy.

29. Plaintiff and the Class Members provided their PII to Defendant, or had their PII provided to Defendant without their knowledge, with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such PII confidential and secure from unauthorized access, including as set forth in AnnieMac's Privacy Policy.

30. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

31. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or

[14] *Id.*

should have known it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

B. AnnieMac Fails to Protect Its Customer's PII—the Data Breach

33. Plaintiff and the proposed Class Members provided their PII to Defendant as a condition of receiving financial mortgage-related services, or who had their PII provided to Defendant without their knowledge in connection with other transactions. Defendant stored Plaintiff's and the Class Members' PII on its computer systems and servers.

34. Unfortunately, Defendant failed to take adequate measures to protect its current and former customers' PII stored on its computer servers, including failing to implement reasonable cybersecurity safeguards or policies to protect PII, and failing to supervise its information technology or data security agents and employees, or vendors, to prevent, detect, and stop breaches of its systems.

35. As a direct result of Defendant's failures, from August 21, 2024, to August 23, 2024, cybercriminals infiltrated Defendant's systems and gained access to, and copied, the PII of AnnieMac's current and former customers, Plaintiff and the Class Members, including but not limited to their names, and Social Security Numbers ("the Data Breach").[15]

36. As admitted by Defendant, AnnieMac would not discover the Data

[15] See Notice of Security Incident, Exhibit A.

Breach until August 23, 2024, when the intrusion had already occurred, and would not notify impacted customers of the Data Breach until months later on November 14, 2024.

37. According to Defendant, AnnieMac discovered the Data Breach on August 23, 2024, when it, "…became aware of suspicious activity on certain systems within [its] network."[16]

38. Only after approximately four (4) months had passed, did Defendant inform its affected customers, Plaintiff and the proposed Class Members, of the Data Breach in its letter dated November 14, 2024, the Data Breach Notice.

39. In the Data Breach Notice, Annie Mac stated that following the discovery of the Data Breach, it secured its systems and conducted an investigation help of "third-party forensic specialists" and "determined that between August 21, 2024, and August 23, 2024, an unknown actor gained access to systems on [its] network and viewed and/or copied certain files from these systems."[17]

40. According to AnnieMac, it then "…identified the affected files and conducted a time-intensive and comprehensive review process of the affected files to identify personal information, the individuals to whom it relates, and address information to be used for notifying impacted individuals."[18]

[16] *Id.*
[17] *Id.*
[18] *Id.*

41. Acknowledging the inadequate security of its systems prior to the Data Breach, Defendant too stated in its Data Breach Notice that following discovery of the intrusion, it "…implemented additional security measures to further protect against similar incidents occurring in the future" and reported the breach to federal and state authorities.[19]

42. Ultimately, AnnieMac encouraged Data Breach victims to "remain vigilant against instances of identity theft and fraud by reviewing account statements and monitoring [their] free credit reports" and informed them of their abilities to place credit freezes and fraud alerts on their credit files.[20]

43. Finally, Defendant offered credit monitoring and identity theft protection services through CyEx to affected customers.[21]

44. On the same date, November 14, 2024, AnnieMac notified the Maine Attorney General of the Data Breach, stating that 171,074 persons were affected, describing the Data Breach as an "External system breach (hacking)" event, but inconsistently stating that the Data Breach was discovered on October 15, 2024.[22]

45. Defendant has obfuscated the details of the Data Breach, omitting from its Data Breach Notice who perpetrated the Data Breach, what deficiencies allowed

---

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] Office of the Maine Attorney General, Data Breach Notifications, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/4e82f3bb-55b2-4dd5-bd97-86893bddd75d.html (last visited Dec. 12, 2024).

cybercriminals to unauthorizedly access customers' PII, why AnnieMac did not immediately detect the intrusion into its systems, why it took Defendant days to notice the cyberattack and Data Breach has occurred, why it took AnnieMac so long to notified impacted customers, and other key details.

46. On information and belief, based on the nature of the cyberattack, Plaintiff's and the members of the proposed Class Members' PII, unauthorizedly disclosed to third-party cybercriminals in the Data Breach, has now been, or will imminently be, posted to the Dark Web for public viewing and use, in the public domain, to be sold and utilized for fraudulent and criminal misuse.

47. As a result of the Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their Social Security numbers. Accordingly, any credit monitoring and identity theft protection which Defendant offered is wholly insufficient to compensate Plaintiff and the Class Members for their damages resulting from the Data Breach.

48. As a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiff and the proposed Class Members have suffered injury and damages, as set forth herein.

C. Plaintiff's Experience

49. Plaintiff was not a customer of AnnieMac, but on information and belief, his PII was provided to Defendant at the time Plaintiff refinanced his

automobile in July or August 2024.

50. Plaintiff is very careful to guard the confidentiality of his PII, and never stores this information in an unsecure setting nor disseminates it publicly.

51. Although Plaintiff never provided his PII to AnnieMac directly, Plaintiff believed that AnnieMac—once in possession of that PII—would adequately safeguard that information, including as set forth in its Privacy Policy, industry standards, and applicable law.

52. Had Plaintiff known that AnnieMac did not utilize reasonable data security measures, Plaintiff would not have entrusted his PII to Defendant.

53. Plaintiff received AnnieMac's Data Breach Notice dated November 14, 2024, informing him that his PII had been accessed, copied, and compromised in the Data Breach, including his name and Social Security Number.[23]

54. As a result of the Data Breach, Plaintiff's PII has been forever compromised.

55. As a direct and proximate result of the Data Breach permitted to occur by Defendant, Plaintiff has suffered, and imminently will suffer, injury-in-fact and damages, including: the unauthorized disclosure of the PII itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be posted on the dark web for sale and used for fraudulent and criminal

[23] *See* Data Breach Notice, Exhibit A.

purposes; as well as misuse of his PII, resulting in a dramatic increase in spam telephone calls, of 5 to 10 calls a day.

56. Plaintiff has not yet signed-up for AnnieMac's complimentary credit monitoring and identity theft protection, but either will do so, or will be forced to spend monies for this necessary protection to mitigate the harms caused by the Data Breach.

57. In addition, because of the Data Breach Plaintiff has been and will be forced to expend considerable time and effort to mitigate the consequences of the unauthorized disclosure of his PII therein, including checking Credit Karma daily, and monitoring his credit files and financial accounts to protect himself from identity theft and fraudulent misuse of his PII unauthorizedly disclosed in the Data Breach.

58. Furthermore, Plaintiff has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his PII in the Data Breach.

59. Plaintiff's sensitive PII remains in Defendant's possession in its computer systems without adequate protection against known threats, exposing Plaintiff to future breaches and additional harm.

60. Further still, because of AnnieMac's Data Breach, its victims, including Plaintiff, face a lifetime risk of identity theft, and increased risk of harm.

D. Defendant's Data Breach Was Foreseeable by Defendant

61. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the Data Breach.

62. Data thieves regularly target institutions like Defendant due to the highly sensitive information in its custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

63. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[24]

64. According to the Identity Theft Resource Center's January 24, 2022, report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)." [25]

65. The increase in such attacks, and attendant risk of future attacks, was

[24] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s/.
[25] *See* Identity Theft Res. Ctr., *2021 Annual Data Breach Report Sets New Record for Number of Compromises* (Jan. 24, 2022), https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises.

widely known to the public and to anyone in Defendant's industry, including AnnieMac. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[26]

66. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members because of a breach.

67. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

68. Defendant was, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

69. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

[26] IBM, *Cost of a Data Breach 2022: A Million-Dollar Race to Detect and Respond*," https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).

70. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

E. Value of Personally Identifiable Information

71. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[28]

72. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[29]

73. For example, PII can be sold at a price ranging from $40 to $200.[30]

---

[27] 17 C.F.R. § 248.201 (2013).
[28] *Id.*
[29] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.
[30] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

Criminals can also purchase access to entire company data breaches from $900 to $4,500.[31]

74. Based on the foregoing, the information compromised in the Data Breach is even more significant because it includes Social Security numbers and other government identification, which is significantly difficult if not impossible to change.

75. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[32]

76. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches

[31] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark.

[32] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

cannot necessarily rule out all future harm.[33]

F. Defendant Failed to Comply with FTC Guidelines

77. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

78. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand its network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts

[33] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

of data being transmitted from the system, and have a response plan ready in the event of a breach.

79. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

80. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet its data security obligations.

81. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

82. Defendant was at all times fully aware of its obligation to protect the PII of consumers under the FTC Act yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

G. Defendant Failed to Comply with Industry Standards.

83. Experts studying cybersecurity routinely identify institutions that store PII like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

84. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Defendant, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, Defendant failed to follow some or all these industry best practices.

85. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring

and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

86. Moreover, a properly trained helpdesk that understands how to face social engineering attacks is an expected part of all cybersecurity programs.

87. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

88. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

H. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

89. Plaintiff and members of the proposed Class have suffered injury and damages from the unauthorized disclosure and misuse of their PII disclosed in the Data Breach that can be directly traced to Defendant, that has occurred, is ongoing, and/or will imminently occur.

90. As stated prior, on information and belief, in the Data Breach, cybercriminals were able to access the Plaintiff's and the proposed Class Members' PII, which is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the Dark Web for sale, causing widespread injury and damages.

91. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

92. Because Defendant failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer injury-in-fact and damages, including but not limited to:

a. The loss of the opportunity to control how PII is used;

b. Unauthorized use of stolen PII;

c. dramatic increase in spam telephone calls;

d. Emotional distress;

e. The compromise and continuing publication of their PII;

f. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

and for necessary credit monitoring and identity theft protection;

g. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

h. The diminution in value of their PII;

i. Delay in receipt of tax refund monies; and,

j. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as AnnieMac fails to undertake the appropriate measures to protect the PII in its possession.

I. The Data Breach Caused Plaintiff and the Class Increased Risk of Identity Theft

93. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

94. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiff's and Class Members' PII falling into the hands of identity thieves.

95. The unencrypted PII of Class Members has already or will end up for sale on the dark web because that is the modus operandi of hackers. Indeed, when

these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and identity theft operations.

96. Further, the standard operating procedure for cybercriminals is to use some data, like the PII here, to access "fullz packages" of that person to gain access to the full suite of additional PII that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.

97. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

98. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

99. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.

100. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.

101. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and

bank/finance fraud.

102. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

103. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

104. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: "For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated."

105. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud

computing, PII is a valuable property right.

106. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PII has considerable market value.

107. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

108. PII are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

109. Where the most PII belonging to Plaintiff and Class Members was accessible from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

110. Thus, Plaintiff and the Class Members must vigilantly monitor their financial and credit accounts for many years to come.

111. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an

individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

112. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

113. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

114. Accordingly, the Data Breach has caused Plaintiff and the proposed

Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein.

115. Defendant knew or should have known of these harms which would be caused by the Data Breach it permitted to occur and strengthened its data systems accordingly.

J. Loss of Time to Mitigate Risk of Identity Theft and Fraud

116. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that his PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

117. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' Social Security numbers or other government identification are affected.

118. By spending this time, data breach Plaintiff was not manufacturing his own harm, she was taking necessary steps at Defendant's direction and because the Data Breach included his Social Security number.

119. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

120. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to his good name and credit record."[34]

K. The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

121. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

[34] See U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

122. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

123. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

CLASS ALLEGATIONS

124. Pursuant to the Federal Rules of Civil Procedure 23(b)(1), 23(b)(3), Plaintiff brings this action on behalf of themselves and on behalf of all members of the proposed class defined as:

> All individuals whose PII was disclosed or compromised in the Data Breach in August 2024, including those persons to whom Defendant sent the Data Breach Notice. ("Class").

125. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as

their immediate family members.

126. Plaintiff reserves the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

127. The proposed Class meets the criteria certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

128. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes approximately 171,074 individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

129. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. When Defendant learned of the Data Breach;

c. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

d. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's conduct violated standards under the FTC Act;

g. Whether Defendant owed duties to Class Members to safeguard their PII;

h. Whether Defendant breached its duties to Class Members to safeguard Plaintiff's and the Class Members' PII, and was negligent;

i. Whether hackers obtained Class Members' PII via the Data Breach;

j. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether implied contracts existed between Defendant and Plaintiff and the Class;

o. Whether Defendant breached implied contracts it had with its customers;

p. In the alternate, whether Defendant was unjustly enriched;

q. Whether Defendant invaded Plaintiff's and the Class Members' privacy;

r. Whether a fiduciary duty existed between Defendant on the one hand and Plaintiff and the Class on the other;

s. Whether Defendant breached its fiduciary duties;

t. Whether Defendant engaged in unfair and deceptive acts and practices in violation of the New Jersey Consumer Fraud Act, N.J.S.A. §§ 56:8-1 *et seq*.;

u. Whether Plaintiff and Class Members are entitled to damages;

v. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

w. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement,

and/or the establishment of a constructive trust.

130. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

131. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

132. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and

desirable advantages of judicial economy.

133. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

134. Class certification is also appropriate. Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

135. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach, as is evident by Defendant's ability to send

those individuals notification letters.

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

136. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

137. Plaintiff and Class Members entrusted their PII to Defendant as a condition of receiving financial mortgage services from AnnieMac, which Defendant then stored on its computer information technology systems and networks.

138. Defendant had full knowledge of the sensitivity of the PII of which it was entrusted, and the types of harm that Plaintiff and the Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that PII.

139. Plaintiff and the Class Members were the foreseeable victims of Defendant's inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their PII in Defendant's possession.

140. By collecting and storing this data in their computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft.

Defendant's duty included a responsibility to implement processes by which it could detect if that PII was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

141. Defendant owed a common law duty of care to Plaintiff and the Class Members to provide adequate data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

142. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

143. Defendant breached its duties, and was negligent, by acts of omission or commission, by failing to use reasonable measures to protect the Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII;

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' PII;

f. Failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

144. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury and damages to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the financial services industry.

145. It was therefore foreseeable that the failure to adequately safeguard Plaintiff's and Class Members' PII would result in one or more types of injuries to them.

146. As a direct and proximate result of Defendant's negligence or negligence *per se*, Plaintiff and Class Members have suffered injury and damages as set forth herein, including but not limited to: loss of the opportunity to control how

PII is used; unauthorized use of stolen PII; dramatic increase in spam telephone calls; emotional distress; compromise and continuing publication of their PII; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud, and for necessary credit monitoring and identity theft protection; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach; diminution in value of their PII; delay in receipt of tax refund monies; continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as AnnieMac fails to undertake the appropriate measures to protect the PII in its possession; and, increased risk of fraud and identity theft.

147. As a result of Defendant's negligence and/or negligence *per se*, Plaintiff and the Class Members are entitled to compensatory, actual, and punitive damages due to the Data Breach.

148. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) properly notify affected victims of the Data Breach (ii) strengthen its data security systems and monitoring procedures; (iii) submit to future annual audits of those systems and monitoring procedures; and (iv) provide adequate credit monitoring to all Class Members.

149. Unless and until enjoined, and restrained by order of this Court,

Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

150. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

151. By collecting the PII of Plaintiff and the Class Members, including in connection with providing financial mortgage services, Defendant impliedly promised to protect their PII through adequate data security measures, as manifested Defendant's conduct, and representations, including those found in AnnieMac's Privacy Policy.

152. The valid and enforceable implied contracts that Plaintiff and Class Members entered into with Defendant included Defendant's promise to protect nonpublic PII given to Defendant from unauthorized disclosures. Plaintiff and Class Members relied upon AnnieMac to protect their PII that had been entrusted to Defendant.

153. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTC Act.

154. Plaintiff and Class Members reasonably believed and expected that Defendant would adequately employ adequate data security to protect that PII. Defendant failed to do so.

155. Under the implied contracts, Defendant promised and was obligated to: protect Plaintiff's and the Class Members' PII that Defendant collected: (i) provided to obtain such services and/or (ii) created in connection therewith. In exchange, Plaintiff and Class Members agreed to pay money for these services and to turn over their PII to Defendant.

156. Both the provision of these services, and the protection of Plaintiff's and Class Members' PII, were material aspects of these implied contracts.

157. Plaintiff and Class Members would not have entrusted their PII to Defendant and entered into these implied contracts with Defendant without an understanding that their PII would be safeguarded and protected, or entrusted their PII to Defendant, in the absence of their implied promise to monitor their computer systems and networks to ensure PII was not disclosed to unauthorized parties and exposed to the public as occurred in the Data Breach.

158. A meeting of the minds occurred when Plaintiff and the Class Members

agreed to, and did, provide their PII to Defendant and paid for services for, amongst other things, (a) the provision of such services and (b) the protection of their PII.

159. Plaintiff and the Class Members performed their obligations under the contracts when their PII was provided to Defendant, or when they paid for financial services.

160. Defendant materially breached its contractual obligations to protect the nonpublic PII of Plaintiff and the Class Members which Defendant required and gathered when the information was unauthorized disclosed in the Data Breach.

161. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

162. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

163. Defendant's conduct as alleged herein also violated the implied

covenant of good faith and fair dealing inherent in every contract.

164. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct, by acts of omission or commission, in breach of these contracts.

165. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class Members did not receive the full benefit of their bargains, and instead received services that were of a diminished value compared to those described in the contracts. Plaintiff and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

166. The injury, losses and damages Plaintiff and Class Members sustained that are described herein were the direct and proximate result of Defendant's breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

167. Plaintiff and the Class Members are entitled to actual, compensatory and consequential, and nominal damages suffered as a result of the Data Breach.

168. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) properly notify affected victims of the Data Breach (ii) strengthen their data security systems and monitoring procedures; (iii) submit to future annual audits of those systems and monitoring procedures; and (iv) provide

adequate credit monitoring to all Class Members.

169. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

170. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

171. Plaintiff brings this claim in the alternate to his claim for Breach of Implied Contract claim.

172. Plaintiff and proposed Class Members conferred benefits upon Defendant in the form of monies paid to AnnieMac, a portion of which was dedicated to adequate data security, and the PII itself.

173. Defendant appreciated or knew of these benefits that it received. And under principles of equity and good conscience, this court should not allow Defendant to retain the full value of these benefits—specifically, the monies, and PII

of Plaintiff and Class Members.

174. After all, Defendant failed to adequately protect Plaintiff's and Class Members' PII. And if such inadequacies were known, then Plaintiff and the members of the Class would never have conferred payment to Defendant, nor disclosed their PII.

175. As a result of Defendant's wrongful conduct as alleged herein, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class Members.

176. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein.

177. As a direct and proximate result of Defendant's unjust enrichment, Plaintiff and Class Members have suffered injury and damages as set forth herein, including but not limited to: loss of the opportunity to control how PII is used; unauthorized use of stolen PII; dramatic increase in spam telephone calls; emotional distress; compromise and continuing publication of their PII; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud, and for necessary credit monitoring and identity theft protection; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach; diminution in value of their PII; delay in receipt of tax refund monies;

continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as AnnieMac fails to undertake the appropriate measures to protect the PII in its possession; and, increased risk of fraud and identity theft.

178. Plaintiff and the Class Members are entitled to compensatory, actual, and punitive damages because of the Data Breach.

179. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to retain the benefits it received, and are still receiving, without justification, from Plaintiff and Class Members in an unfair, unconscionable, and oppressive manner. Defendant's retention of such funds under circumstances making it inequitable to do so constitutes unjust enrichment.

180. The financial benefits derived by Defendant rightfully belong to Plaintiff and Class Members. Defendants should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all wrongful or inequitable proceeds collected by Defendant. A constructive trust should be imposed upon all wrongful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

181. Plaintiff and the Class Members have no adequate remedy at law.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

182. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

183. Plaintiff and the Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

184. Defendant owed a duty to Plaintiff and the Class Members to keep their PII confidential.

185. Defendant failed to protect said PII and exposed the PII of Plaintiff and the Class Members to unauthorized persons in the Data Breach.

186. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiff and the Class Members, by way of Defendant's failure to protect the PII.

187. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class Members is highly offensive to a reasonable person.

188. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff's and the Class Members' PII was disclosed to Defendant in connection with receiving financial mortgage loan services, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable in their

belief that such information would be kept private and would not be disclosed without their authorization.

189. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and the Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, or private quarters, of a kind that would be highly offensive to a reasonable person.

190. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its data security practices were inadequate and insufficient.

191. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when they allowed improper access to its systems containing Plaintiff's and Class Members' PII.

192. Defendant was aware of the potential of a data breach and failed to adequately safeguard their systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PII.

193. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

194. Moreover, given the ubiquitous nature of data breaches, Defendant was substantially certain that choosing to forego reasonable cybersecurity standards for

lead to a data breach and its inherent harms to Defendant's consumers.

195. Indeed, in addition to the intrusion upon seclusion, Defendant's actions and failures amount to a public disclosure of private facts as the disclose of data here is highly offensive to any reasonable person and was published to cybercriminals and identity thieves who are in a special relationship with Plaintiff and the proposed Class Members in that those cybercriminals and identity thieves are precisely the individuals from whom the required safeguards are meant to protect Plaintiff and the Class.

196. As a direct and proximate result of the Defendant's invasion of privacy—intrusion into seclusion, Plaintiff and Class Members have suffered injury and damages as set forth herein, including but not limited to: loss of the opportunity to control how PII is used; unauthorized use of stolen PII; dramatic increase in spam telephone calls; emotional distress; compromise and continuing publication of their PII; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud, and for necessary credit monitoring and identity theft protection; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach; diminution in value of their PII; delay in receipt of tax refund monies; continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as AnnieMac fails to undertake

the appropriate measures to protect the PII in its possession; and, increased risk of fraud and identity theft.

197. Plaintiff and the Class Members are entitled to compensatory, actual, and punitive damages as a result of the Data Breach.

198. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) properly notify affected victims of the Data Breach (ii) strengthen its data security systems and monitoring procedures; (iii) submit to future annual audits of those systems and monitoring procedures; and (iv) provide adequate credit monitoring to all Class Members.

199. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

200. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

201. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

202. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of AnnieMac's relationship with its customers, in particular, to keep secure their PII.

203. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII; failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and Class Members' PII; failing to adequately train employees on proper cybersecurity protocols; failing to adequately monitor the security of its networks and systems; failure to periodically ensure that their network system had plans in place to maintain reasonable data security safeguards; allowing unauthorized access to Plaintiff's and Class Members' PII; and by failing to timely notify Plaintiff and Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity

theft and other damages.

204. As a direct and proximate result of the Defendant's breach of fiduciary duty, Plaintiff and Class Members have suffered injury and damages as set forth herein, including but not limited to: loss of the opportunity to control how PII is used; unauthorized use of stolen PII; dramatic increase in spam telephone calls; emotional distress; compromise and continuing publication of their PII; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud, and for necessary credit monitoring and identity theft protection; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach; diminution in value of their PII; delay in receipt of tax refund monies; continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as AnnieMac fails to undertake the appropriate measures to protect the PII in its possession; and, increased risk of fraud and identity theft.

205. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses, such as the invasion of their privacy rights.

206. As a direct and proximate result of Defendant's breach of fiduciary

duty, Plaintiff and the Class Members are entitled to compensatory, actual, and punitive damages because of the Data Breach.

COUNT VI
VIOLATIONS OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J.S.A. § 56:8-1, *et seq.*
(On Behalf of Plaintiff and the Class)

207. Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

208. Plaintiff and the Class Members, and Defendant are each a "person" within the meaning of the New Jersey Consumer Fraud Act ("NJCFA"). N.J.S.A. § 56:8-1(d).

209. At all relevant times, Defendant was engaged in the advertising and sale of merchandise and services, as those terms are defined in the NJCFA. N.J.S.A. *See* § 56:8-1.

210. Under the NJCFA, the "act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise . . . or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice." N.J.S.A. § 56:8-2.

211. The NJCFA further forbids the "advertisement of merchandise as part of a plan or scheme not to sell the item or service so advertised." N.J.S.A. § 56:8-2.2.

212. As set forth herein, Defendant engaged in unfair and deceptive acts or practices, including but not limited to:

a. Failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff's and Class Members's PII;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members's PII, including duties imposed by Section 5 of the FTC Act;

c. Failing to properly protect the integrity of the systems containing Plaintiff's and Class Members's PII;

d. Failing to prevent the unauthorized access or disclosure of Plaintiff's and Class Members's PII;

e. Failing to timely disclose the Data Breach to Plaintiff and Class Members;

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff 'and Class Members's PII, including that it would "…restrict access to nonpublic personal information about you to those employees who need to know that information to provide products or services to you…" that it would "…maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic personal information" and that AnnieMac would "use industry-standard methods to protect your personally identifiable information from unauthorized access."[35]

g. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members's PII, including duties imposed by Section 5 of the FTCA;

h. Omitting, suppressing, and concealing the material fact that they did not properly secure Plaintiff's and Class Members's PII;

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII,

[35] *Privacy Policy*, Exhibit B.

including duties imposed by Section 5 of the FTC Act; and

j. Overcharging for services provided without adequate data security measures in place.

213. Defendant knowingly represented they would protect Plaintiff's and Class Members's PII despite not having adequate protections in place to induce Plaintiff and Class Members to purchase their financial services.

214. Defendant's concealments, omissions, and false promises induced Plaintiff and Class Members to purchase Defendant's services.

215. But for these unlawful acts by Defendant, Plaintiff and Class Members would not have entrusted Defendant with their PII.

216. Defendant engaged in unfair or deceptive acts in violation of the NJCFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiff's and Class Members' PII in a manner that complied with applicable laws, regulations, and industry standards, as they represented they would.

217. As a direct and proximate result of the Defendant's unfair acts and practices, Plaintiff and Class Members have suffered injury and damages and ascertainable loss of money and property as set forth herein, including but not limited to: loss of the opportunity to control how PII is used; unauthorized use of stolen PII; dramatic increase in spam telephone calls; emotional distress; compromise and

continuing publication of their PII; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud, and for necessary credit monitoring and identity theft protection; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach; diminution in value of their PII; delay in receipt of tax refund monies; continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as AnnieMac fails to undertake the appropriate measures to protect the PII in its possession; and, increased risk of fraud and identity theft.

218. As a direct and proximate result of Defendant's unfair acts and practices in violation of the NJCFA, pursuant to N.J.S.A. § 56:8-19, Plaintiff and the proposed Class Members are entitled to recover actual damages, treble damages, and reasonable attorneys' fees.

219. Further, Plaintiff and the Class Members seek all other relief as allowed by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff individually and on behalf of all others similarly situated, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying this action as a class action and appointing Plaintiff as Class Representative and appointing his counsel to represent the Class;

B. For an award of actual damages, compensatory damages, nominal damages, and statutory treble damages under N.J.S.A. § 56:8-19, in an amount to be determined according to proof;

C. For punitive damages, as permitted by law;

D. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

E. For injunctive relief requested by Plaintiff, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification

for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of

Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

x. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xi. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance

with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xiv. for a period of 7 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

F. For an award of attorneys' fees under the common fund doctrine, as well as reasonable attorneys' fees under N.J.S.A. § 56:8-19

G. For Plaintiff's costs, and any other expenses, including expert witness

fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: December 13, 2024

Respectfully submitted,

/s/ James E. Cecchi

James E. Cecchi
CARELLA BYRNE CECCHI BRODY & AGNELLO, P.C.
5 Becker Farm Road
Roseland, New Jersey 07068
(973) 994-1700
jcecchi@carellabyrne.com

J. Gerard Stranch, IV (*pro hac vice forthcoming*)
Andrew E. Mize (*pro hac vice forthcoming*)
Grayson Wells (*pro hac vice forthcoming*)
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
gstranch@stranchlaw.com
amize@stranchlaw.com
gwells@stranchlaw.com

Counsel for Plaintiff and the Proposed Class